Papéis e Responsabilidades Para Planejamento de Contingência

Versão 1

Julho 2008

Dr Gary Hinson PhD CISSP MBA
CEO of IsecT Ltd.

E

Larry Kowalski CISSP ITIL
Cybersecurity DR Program Office, IRS

(Traduzido para o Português do Brasil por Luiz Chalola)

Sumário Executivo

Com base nos padrões da série ISO/IEC 27000 e outras referências, este documento descreve as responsabilidades e competências comumente associadas às funções de planejamento de contingência, continuidade de negócios, retomada de negócios e recuperação de desastres de TI em grandes organizações do setor público ou privado. Embora as funções sejam frequentemente combinadas e simplificadas em organizações menores, princípios amplamente semelhantes geralmente se aplicam.

Conteúdo

Seção *Página*

1 Introdução 3

1.1 Histórico, conceitos e termos-chave 3

1.2 Escopo e aplicabilidade deste documento 4

1.3 Utilizando este documento - uma advertência importante 5

2 Planejamento de Contingência (PC) papéis e responsabilidades 5

2.1 Gerente de Planejamento de Contingência 5

2.2 Gerente de Conformidade de Planos de Contingência 6

O Gerente de Conformidade de Planos de Contingência dá suporte ao Gerente de Planos de Contingência em ambos os papéis demonstrando e alcançando a conformidade com as políticas de PC, estratégias, padrões, etc. 6

2.3 Escritório de PC 6

3 Papéis e responsabilidades de Planejamento de Continuidade de Negócios (PCN) e Planejamento de Retorno de Negócios (PRN) 7

3.1 Gerente de Planejamento de Continuidade de Negócios 7

3.2 Gerenciamento de PRN 8

3.3 Escritório de PCN / PRN 9

4 Papéis e responsabilidades do Planejamento de Recuperação de Desastres de TI 10

4.1 Gerente de Recuperação de Desastres de TI I 10

4.2 Gerente de Conformidade de RD de TI 10

4.3 Coordenador de Testes e Exercícios de Recuperação de Desastres de TI 11

4.4 Gerente de Desenvolvimento e Avaliação Técnica de PRD de TI 12

4.5 Escritório de RD de TI 12

5 Outros papéis e responsabilidades relacionados ao PC 13

5.1 Papéis de Gerenciamento de Incidentes 13

5.2 Papéis de Gerenciamento de Crise 14

5.3 Encarregados de Gerenciamento de Incidentes e Crises, planejamento de sucessão e rotação de trabalho 14

5.4 Proprietários de Ativos de Informação (IAOs) 14

5.5 Custodiantes 15

5.6 Funções operacionais de Continuidade de Negócios 15

5.7 Funções das Operações de RD de TI 15

6 Referências e leituras adicionais 17

7 Comentários sobre este documento 17

8 Agradecimento 17

Este documento foi baseado em um excelente documento de estratégia de treinamento em RD, gentilmente fornecido por Larry Kowalski, do Escritório de Programas de RD de Segurança Cibernética da Receita Federal dos EUA. Gary Hinson reformatou e ampliou ligeiramente o documento para os propósitos do kit de ferramentas ISO27k, mas permanece extremamente grato pela generosa contribuição intelectual que motivou este trabalho. Obrigado Larry! 17

Aviso de direitos autorais e isenção de responsabilidade 17

1 Introdução

1.1 Histórico, conceitos e termos-chave

A base fundamental do Planejamento de Contingência (PC) é que, desde que todos os riscos não podem ser totalmente eliminados na prática, os riscos residuais sempre permanecem. Apesar dos melhores esforços da organização para evitá-los, preveni-los ou mitigá-los, os incidentes ainda ocorrerão.Situações particulares, combinações de eventos adversos ou ameaças e vulnerabilidades imprevistas podem conspirar para contornar ou sobrecarregar até mesmo os melhores controles de segurança da informação projetados para garantir a confidencialidade, integridade e disponibilidade dos ativos de informação.

No contexto deste documento, PC é definido como a totalidade das atividades, controles, processos, planos etc. relativos a grandes incidentes e desastres. É o ato de se preparar para grandes incidentes e desastres, formular planos flexíveis e ordenar os recursos adequados que entrarão em ação no evento, seja o que for. A própria palavra "contingência" implica que as atividades e recursos que serão necessários após grandes incidentes ou desastres são contingentes (dependem) da natureza exata dos incidentes e desastres que realmente se desenrolam. Nesse sentido, o PC envolve a preparação para o inesperado e o planejamento para o desconhecido.

O propósito básico do PC é minimizar as consequências ou impactos adversos de incidentes e desastres. Dentro do campo do PC, uma série de termos e atividades mais específicos são distinguidos neste documento e formam a base dos papéis identificados abaixo:

- **As práticas de gerenciamento de disponibilidade e planejamento de continuidade** envolvem medidas de resiliência projetadas para manter os processos de negócios essenciais e a infraestrutura de TI de suporte funcionando, apesar de incidentes e desastres (limitados):

    - **Planejamento de Continuidade de Negócios (PCN)** envolve medidas para garantir, na medida do possível, que os processos críticos de negócios continuem a operar satisfatoriamente, apesar de uma ampla gama de incidentes. Isso inclui aspectos como executar atividades paralelas em locais díspares, usar suplentes, ter fornecedores alternativos etc.;
    - **Planejamento de Continuidade de TI (PCTI)** envolve medidas para garantir que, na medida do possível, os sistemas de TI, redes e infraestrutura e processos associados que suportam processos de negócios críticos permaneçam em operação apesar de desastres. Isso inclui aspectos como projetos e configurações de sistema/rede tolerantes a falhas, resilientes ou de alta disponibilidade, redundância integrada e failover automatizado dos sistemas de TI de suporte, gerenciamento de capacidade e desempenho etc.

- **Planejamento de Recuperação e Retomada** refere-se à recuperação ou retomada de negócios e operações de TI após incidentes e desastres, normalmente de locais alternativos, usando equipamentos de reserva, etc.:

▪ **Planejamento de Retomada de Negócios (PRN)** envolve o planejamento para retornar ou restaurar processos de negócios críticos e importantes para algo próximo da normalidade após desastres ou incidentes graves que sobrecarregam os recursos de resiliência mencionados acima. Isso inclui atividades como realocação de funcionários para locais alternativos de escritório, processamento manual de retorno, relaxamento de divisões de responsabilidade e autoridades delegadas, etc .;

- **Planejamento de Recuperação de Desastres de TI (PRDTI)** envolve o planejamento para recuperação de sistemas e serviços de TI críticos em uma situação de fallback após um desastre que sobrecarrega os arranjos de resiliência; exemplos incluem a restauração manual de sistemas de TI e dados em equipamentos alternativos/em espera de backups ou arquivos, utilizando instalações de comunicação de emergência, etc .

- **As atividades de gerenciamento de crises e incidentes** são focadas em gerenciamento de incidentes e cenários de desastre “ao vivo” assim que eles ocorrem:

  - **Gerenciamento de Incidentes (GI)** envolve atividades e processos destinados a avaliar e responder a incidentes relacionados à segurança da informação de todos os tipos. A maioria das atividades de Gerenciamento de Incidentes são rotineiramente exercitadas no curso normal de negócios, lidando com todos os tipos de incidentes menores. Os processos proativos de Gestão de Incidentes de melhores práticas incorporam o “aprendizado corporativo” por meio da atualização contínua dos processos, sistemas e controles e melhoria da resiliência e das atividades de recuperação em resposta a incidentes e catástrofes reais e a quase incidentes.

  - **Gerenciamento de Crises (GC)** envolve atividades de gestão de emergência associadas à gestão de grandes incidentes e crises, principalmente relacionadas com aspectos de saúde e segurança. As principais atividades na fase de crise incluem tipicamente a avaliação preliminar da situação, a ligação com os serviços de emergência e gestão, e (no caso de incidentes graves) a invocação de Planejamento de Retomada de Negócios (PRN) e Recuperação de Desastres de TI. A rápida formação de um grupo/equipe competente de gestão de crises para gerir e controlar as atividades de recuperação em curso é um elemento importante do GC.

É importante apreciar que o planejamento e a preparação são fundamentais para todas as atividades relacionadas com o PC. Enquanto muitos de nós antecipamos ser capazes de lidar e ultrapassar situações de crise até certo ponto em tempo real, o PC pretende preparar planos adequados e armazenar recursos essenciais antes de qualquer crise para tornar a situação mais controlável e menos perturbadora no dia. Além disso, embora seja sensato preparar-se minuciosamente para incidentes comuns (tais como interrupções de energia ou serviços de telecomunicações), o verdadeiro PC inclui um elemento de preparação para eventos totalmente imprevistos, por exemplo, pré-determinar a estrutura e os processos de gestão de crise para avaliar e reagir adequadamente a qualquer incidente de forma mais eficiente do que se tais preparativos não tivessem sido feitos.

1.2 Escopo e aplicabilidade deste documento

Os papéis e responsabilidades específicas identificadas neste documento aplicam-se primeiramente à grandes organizações tais como multinacionais no setor privado ou grandes departamentos governamentais. Grandes organizações possuem tanto a disponibilidade de recursos quanto os requisitos para justificar a alocação de profissionais dedicados todo o tempo as tarefas associadas ao Planejamento de Contingência. As pequenas e médias empresas desempenham tipicamente funções semelhantes utilizando menos indivíduos, muitos dos quais podem trabalhar em tempo parcial em determinados elementos do Planejamento de Contingência e podem ou não ser tão altamente qualificados. No extremo, as microempresas com apenas um

pequeno punhado de empregados podem atribuir todas as responsabilidades do Planejamento de Contingência a um único empregado, embora idealmente com um adjunto ou eventual substituto.

Com a devida consideração pela gerência e adaptação para adequação aos requisitos específicos, as descrições de atividades chave e competências neste documento podem ser usadas para o desenvolvimento de descrições de funções, avisos de vagas, etc para papéis relacionados ao PC. Na prática as organizações que mais se aproximam da descrição de âmbito acima, já definiram uma série de papéis relacionados ao PC, mas podem não ter tido em conta toda a gama de atividades aqui descritas, o que significa que alguma revisão e atualização de descrição de funções podem estar de acordo. Outras organizações têm menos probabilidades de possuírem uma abordagem tão abrangente do PC e podem também beneficiar-se da revisão de suas estruturas de governança e descrições de funções, analisando particularmente quaisquer lacunas signficativas na cobertura.

1.3 Utilizando este documento - uma advertência importante

Este documento é fornecido apenas para fins de informação e discussão. Os papéis e competências explicadas no resto deste documento são genéricos. É pouco provável que o documento preencha quaisquer requisitos específicos da organização sem alguma adaptação e personalização que possa ser extensa. **Os leitores são encorajados a fazer uso das referências e outras leituras listadas no final, e/ou a recorrer a funcionários ou consultores qualificados e competentes com experiência em PC para darem corpo aos detalhes.** Favor ler o aviso de direitos de autor e a declaração de exoneração de responsabilidade para mais informações. As competências abaixo referidas referem-se a três "níveis" de conhecimento e perícia em vários tópicos, nomeadamente: conhecimento especializado (o nível de conhecimento esperado de um perito na área com pelo menos dez anos de experiência de trabalho e qualificações relevantes); conhecimento detalhado (entre perito mas e conhecimento de trabalho, talvez apoiado por qualificações relevantes); e conhecimento de trabalho (esperado de alguém com pelo menos um ou dois anos de experiência de trabalho na área).

2 Planejamento de Contingência (PC) papéis e responsabilidades

2.1 Gerente de Planejamento de Contingência

Embora a maioria das atividades relacionadas com a PC recaiam nas funções subsidiárias individuais listadas abaixo, existe geralmente a necessidade de um gestor de mais alto nível para gerir, dirigir e controlar as atividades do PC como um todo.

*2.1.1 **Atividades Chave:***

- Estabelecer ligações entre coordenando várias partes interessadas internas e externas (tais como gestores de mais alto nível, principais clientes, fornecedores e parceiros comerciais, representantes dos empregados e fornecedores de serviços/equipamentos de terceiros) para elucidar os requisitos e capacidades do PC, utilizando processos racionais de Análise de Impacto de Negócios (AIN) para 'normalizar' e dar prioridade aos requisitos do PC em nome da organização como um todo, e formar o quadro geral dos requisitos do PC em relação às atividades operacionais e estratégicas normais;
- Identificar falhas de financiamento e progresso, ou riscos não geridos que ameacem o sucesso das atividades do PC, e trabalhar com a gestão para abordar e resolver estas questões;
- Ter uma visão estratégica do PC em toda a empresa, desenvolvendo estratégias e políticas amplas para o PC que complementem e apoiem outras estratégias comerciais rotineiras, objetivos de gerenciamento de risco e segurança, políticas de RD de TI, etc;

- Implementar os mecanismos adequados de gerenciamento, controle, diretiva e monitoramento para governar as atividades de PC (com uma grande equipe de PC, isso provavelmente incluirá entrevistas e nomeação de vários gerentes, coordenadores, líderes de equipe etc. para liderar as diversas atividades de PC).

2.1.2 Competências:

- Conhecimento Especializado de PC
- Conhecimento detalhado da estrutura de gestão da organização, estratégias comerciais, etc.;
- Conhecimento de trabalho de gerenciamento de projetos, PCD / PRD de TI, etc.
- Demonstrar habilidades de liderança;
- Habilidade de comunicar-se calmamente, efetivamente e com autoridade, inclusive em uma crise.

2.2 Gerente de Conformidade de Planos de Contingência

O Gerente de Conformidade de Planos de Contingência dá suporte ao Gerente de Planos de Contingência em ambos os papéis demonstrando e alcançando a conformidade com as políticas de PC, estratégias, padrões, etc.

2.2.1 - Atividades Chave

- Gerenciar relatórios de gerenciamento de rotina de PC, extraindo informações relevantes de AINs, planos, incidentes, desastres, exercícios, etc., além do contexto mais amplo dos órgãos legais, reguladores e de normalização (por exemplo, mudanças legislativas);
- Desenvolver e ajudar a realizar atividades de treinamento e conscientização do PC*;*
- Auxiliar no planejamento de AIN e e teste/exercício, determinando quaisquer requisitos de conformidade associados (por exemplo, obrigações legais de conduzir um certo número e tipo de exercício a cada ano).

2.2.2 Competências

- Conhecimento detalhado do PC, idealmente evidenciado por qualificações e experiência relevantes;
- Conhecimento detalhado das políticas corporativas, leis e regulamentos que regem o PC;
- Conhecimento detalhado do processo e requisitos de Certificação e Credenciamento (C&A) [quando relevante];
- Experiência profissional em processos comerciais críticos e prioridades relativas;
- Capaz de articular e explicar as políticas de PC em termos operacionais, e identificar as necessidades de treinamento e conscientização de PC, além de métodos de treinamento e conscientização com boa relação custo-benefício;
- Capaz de desenvolver, medir e relatar métricas de PC adequadas Redação comercial, apresentação e habilidades de comunicação relacionadas.

2.3 Escritório de PC

Assim como o Gerente de Incidentes, Coordenador de Crise, Gerente de PCN, Gerente de PRN, Gerente de PRD de TI e outros, o Gerente de PC em grandes organizações pode ser apoiado por

um Escritório de Gerenciamento de PC dedicado e/ou funções subsidiárias que fornecem suporte de gerenciamento de projetos a outras funções relacionadas a PC, tais como PCN e PRD de TI.

2.3.1 Atividades Chave:

- Ajudar a construir um 'centro de excelência' para o PC - um ponto focal na organização oferecendo apoio e direção interna de consultoria em assuntos de PC com a ajuda dos gerentes da BC/BR e outros especialistas;
- Projetar e construir inventários de processos críticos, suporte a sistemas de TI, etc;
- Programar e organizar reuniões para os gerentes de PC com os Proprietários dos Ativos de Informação (IAOs) e outros colaboradores;
- Orientar e apoiar a criação de planos de contingência razoavelmente consistentes, abrangentes e de alta qualidade em toda a empresa, particularmente no que diz respeito aos processos comerciais críticos e às funções de apoio/ capacitação associadas;
- Auxiliar na elaboração de políticas, normas, procedimentos e diretrizes relacionadas à PC;
- Executar ou apoiar outros na identificação e gestão de riscos relacionados a projetos de PC;
- Auxiliar na criação de solicitações/propostas de orçamento, casos de negócios, etc., para diversas atividades de PC;
- Monitorar e preparar relatórios gerenciais sobre os planos relacionados a PC, o progresso dos planos, orçamentos, riscos e oportunidades;
- Ajudar na coordenação e/ou na realização de atividades de conscientização, treinamento e educação, exercícios/testes relacionados à PC, etc.
- Ajudar em uma crise a implementar planos de PC, abordar questões operacionais, comunicar clara e efetivamente, etc

2.3.2 Competências:

- Experiência profissional em PC, CN, RN, PRD TI etc;
- Capaz de construir e manter relações de trabalho produtivas com outros empresários;
- Habilidades administrativas gerais, com alguma exposição ao gerenciamento de projetos, métricas/relatórios de gerenciamento, etc;
- Um olho para os detalhes, suficientemente diligente, persistente e eficiente para completar adequadamente as atividades designadas dentro de prazos realistas;
- Capaz de se comunicar com calma, eficácia e autoridade, inclusive em uma crise;

3 Papéis e responsabilidades de Planejamento de Continuidade de Negócios (PCN) e Planejamento de Retorno de Negócios (PRN)

3.1 Gerente de Planejamento de Continuidade de Negócios

O foco principal do Gerente de Planejamento de Continuidade de Negócios é garantir que os processos críticos de negócios sejam suficientemente resistentes para continuar operando efetivamente, apesar dos incidentes.

3.1.1 Atividades Chave:

- Gerenciar o processo global de Planejamento de Continuidade de Negócios;
- Aconselhar e assistir IAOs, gerentes de PRN / PRD TI e outros com assuntos de PCN;
- Avaliar e priorizar os processos comerciais a partir da perspectiva da resiliência / disponibilidade;
- Determinar/especificar os requisitos de resiliência, levando em conta as interdependências entre os processos e os aspectos de suporte dos sistemas de TI, e preparar planos de CN
- Ajudar a justificar qualquer investimento adicional necessário nos acordos da Continuidade de Negócios, ajudando a preparar propostas de investimento, casos comerciais, propostas de orçamento, etc..;
- Assegurar que os planos da CN sejam preparados para um nível consistente de qualidade, precisão, completude e detalhe, normalmente através da preparação de modelos adequados.

3.1.2 ***Competências:***

- Conhecimento especializado de PCN;
- Conhecimento detalhado de PRN;
- Experiência profissional nos processos críticos de negócios, políticas, apetite de risco,etc..;
- Experiência profissional de PC e PRD de TI;
- Conhecimento prático das práticas de gestão de investimentos/finanças da organização.
- Capaz de se comunicar com calma, eficácia e autoridade, inclusive em uma crise.

3.2 Gerenciamento de PRN

O papel do Gerente do PRN enfatiza a restauração oportuna dos processos comerciais após um desastre

3.2.1 ***Atividades Chave:***

- Gerenciar o processo geral do PRN;
- Colaborar com IAOs, PCN e colegas de PRD TI em assuntos de PRN;
- Avaliar e priorizar os processos comerciais a partir da perspectiva da recuperação;
- Determinar os requisitos de recuperação, levando em conta as interdependências entre os processos e os aspectos de suporte dos sistemas de TI;
- Justificar qualquer investimento adicional necessário no PRN;
- Preparar Planos de RN.

3.2.2 Competências:

- Conhecimento especializado em PRN;
- Conhecimento detalhado de PCN;
- Experiência profissional dos processos críticos de negócios da organização;
- Experiência profissional de PC e PRD de TI ;

- Capaz de desenvolver casos comerciais sólidos;
- Capaz de se comunicar com calma, eficácia e autoridade, inclusive em uma crise.

3.3 Escritório de PCN / PRN

Dependendo da quantidade de trabalho envolvido, os Gerentes do PCN e do PRN podem precisar do apoio de uma equipe administrativa. [Nota: o escritório do PCN/PRD pode fazer parte do escritório do PC acima mencionado].

3.3.1 Atividades Chave:

- Ajudar a construir um 'centro de excelência' para a CN / RN - um ponto focal na organização oferecendo apoio e direção interna de consultoria em assuntos da CN / RN com a ajuda dos gerentes da CN / RN e outros especialistas;
- Manter inventários de processos críticos, sistemas de suporte de TI e etc.;
- Programar e organizar reuniões para seus gerentes com os Proprietários dos Ativos de Informação e outros colaboradores;
- Orientar e apoiar a criação de planos PC/RN razoavelmente consistentes, abrangentes e de alta qualidade em toda a empresa, particularmente no que diz respeito aos processos comerciais críticos e às funções de apoio /capacitação associadas;
- Auxiliar na elaboração de políticas, normas, procedimentos e diretrizes relacionadas à CN / PN;
- Executar ou apoiar outros na identificação e gestão de riscos relacionados a projetos CN/RN;
- Auxiliar na criação de solicitações/propostas de orçamento, casos de negócios, etc., para diversas atividades da CN/RN;
- Monitorar e preparar relatórios gerenciais sobre os planos relacionados à CN/RN, o progresso dos planos, orçamentos, riscos e oportunidades;
- Ajudar na coordenação e/ou na realização de atividades de conscientização, treinamento e educação relacionadas à CN/RN, exercícios/testes, etc;
- Ajudar em uma crise a implementar planos CN/RN abordar questões operacionais, comunicar clara e efetivamente, etc.

3.3.2 Competências:

- Experiência profissional de CN, RN, PC, PRD IT *etc*.;
- Capaz de construir e manter relações de trabalho produtivas com outros funcionários;
- Habilidades administrativas gerais, com alguma exposição ao gerenciamento de projetos, métricas/relatórios de gerenciamento, etc;
- Um olho para os detalhes, suficientemente diligente, persistente e eficiente para completar adequadamente as atividades designadas dentro de prazos realistas;
- Capaz de se comunicar com calma, eficácia e autoridade, inclusive em uma crise.

4 Papéis e responsabilidades do Planejamento de Recuperação de Desastres de TI

4.1 Gerente de Recuperação de Desastres de TI I

O Gerente de Recuperação de Desastres de TI tem responsabilidades gerais pela gestão e direção do PRD de TI.

*4.1.1 **Atividades Chave***

- Coordena a participação das partes interessadas no planejamento de DR e trabalha com os Proprietários dos Ativos de Informação para priorizar os processos comerciais críticos;
- Gerencia os recursos dos programas de RD;
- Definir os princípios, políticas e procedimentos necessários para apoiar ou reconstituir funções comerciais essenciais após um evento catastrófico;
- Desenvolver programas de avaliação de impacto de negócios, conformidade, treinamento, testes e exercícios, avaliação técnica e desenvolvimento de planos;
- Implementar políticas de RD através de acordos de RD, tais como backups regulares de dados; arquivo seguro de dados; restauração de backup; armazenamento seguro de mídia de backup dentro e fora do local; fornecimento de instalações alternativas de processamento de TI, redes, etc.
- Avaliar o programa geral de PRD de TI e o estado de prontidão da TI em relação ao PRN e às exigências mais amplas da PC.

4.1.2 Competências

- Conhecimento especializado em PRD TI;
- Conhecimento detalhado de sistemas de TI, redes e aplicações que suportam processos críticos de negócios;
- Conhecimento detalhado de gerenciamento de projetos;
- Experiência profissional de PC, PCN e PRN;
- Experiência profissional dos processos críticos de negócios;
- Experiência profissional de certificação e acreditação de processos [em situações onde o PD de TI tem que ser avaliados e certificados de forma independente em relação a critérios de toda a empresa e, em alguns casos, às obrigações legais/regulamentares;
- Capaz de contribuir proativamente na Análise de Impacto de Negócios;
- Capaz de se comunicar com calma, eficácia e autoridade, inclusive em uma crise.

4.2 Gerente de Conformidade de RD de TI

O Gerente de Conformidade de RD de TI apoia o Gerente de PDR de TI a alcançar e demonstrar conformidade com as políticas de RD de TI

4.2.1 Atividades Chave:

- Gerenciar relatórios de RD TI de rotina, extraindo informações relevantes de AINs, planos, incidentes, desastres, exercícios, etc., além do contexto mais amplo dos órgãos legais, reguladores e de normalização (por exemplo, mudanças legislativas);
- Auxiliar na realização de atividades de treinamento e conscientização de TI RD;

- Auxilia na AIN e no planejamento de testes/exercícios, determinando quaisquer requisitos de conformidade associados (por exemplo, obrigações legais de conduzir um determinado número e tipo de exercício a cada ano).

4.2.2 Competências

- Conhecimento detalhado de práticas de conformidade;
- Conhecimento detalhado das políticas corporativas, leis e regulamentos que regem o PRD de TI;
- Conhecimento detalhado do planejamento de RD TI como disciplina, idealmente evidenciado por qualificações e experiência relevantes;
- Conhecimento detalhado do processo e requisitos de Certificação e Credenciamento (C&A) [quando relevante]
- Experiência profissional de processos críticos de negócios e prioridades relacionadas;
- Capaz de articular e explicar as políticas de RD de TI em termos operacionais;
- Capaz de colaborar na entrega de treinamento e conscientização de RD de TI;
- Redação comercial, apresentação e habilidades de comunicação relacionadas.

4.3 Coordenador de Testes e Exercícios de Recuperação de Desastres de TI

O Coordenador de Testes e Exercícios de Recuperação de Desastres de TI auxilia o Gerente de Recuperação de Desastres de TI a projetar e conduzir testes, conscientização, treinamento e processos educacionais associados ao Planejamento de Recuperação de Desastres de TI de acordo com as exigências legais, regulamentares e comerciais para garantia das atividades chave de Planejamento de Contingência

4.3.1 Atividades chaves:

- Projetar, planejar/agendar e coordenar testes de Planejamento de Recuperação de Desastres de TI(principalmente focados em testar o funcionamento correto das tecnologias Recuperação de Desastres) e exercícios (principalmente focados no treinamento de pessoas em procedimentos e atividades relacionadas a Recuperação de Desastres de TI), avaliando sua eficácia e promovendo quaisquer atividades de melhoria que sejam consideradas necessárias para atender aos objetivos do Planejamento de Contingência;
- Gerenciar os recursos necessários para testes e exercícios;
- Dividir a responsabilidade entre o Gerente de Plano de Recuperação de Desastres de TI, Escritório de Recuperação de Desatres de TI, vários profissionais de TI, proprietários de ativos de informação, gerentes de Continuidade de Negócios e Recuperação de Desastres etc. sobre todos os assuntos relacionados aos testes e exercícios de Planos de Recuperação de Desastres de TI, incluindo planejamento, execução e relatórios gerenciais. Ele/ela coordena a TI e outros recursos necessários, e avalia a eficácia dos testes e exercícios de DR de TI, fornecendo feedback construtivo.

4.3.2 Competências:

- Conhecimento detalhado de leis, regulamentos e requisitos de negócios em relação às exigências de garantia do Planejamento de Contingência para comprovar os elementos do Planejamento de Contingência em termos de Planejamento de Recuperação de Desastres de TI para comprovar os elementos do Planejamento de Contingência em termos de Planejamento de Recuperação de Desastres de TI;

- Experiência profissional em controles de segurança da informação relacionados ao Planejamento de Continuidade e Planejamento de Recuperação de Desastres;
- Experiência Profissional de processos críticos de negócios e suas prioridades relacionadas;
- Experiência Profissional de processos de Certificação e Aceitação (quando relevantes);
- Capaz de projetar planos de teste/exercício de PRD de TI, cenários e métricas;
- Capaz de programar, gerenciar e entregar o programa de teste/exercício de RDP de TI;
- Habilidade em projetar testes/exercícios de RD de TI eficazes que forneçam o nível desejado de garantia, minimizando custos e riscos desnecessários de testes;
- Capaz de coordenar as atividades de várias partes interessadas e participantes em cenários de teste/exercício;
- Capacidade analítica para avaliar os resultados dos exercícios e testes de RD de TI em relação às expectativas.

4.4 Gerente de Desenvolvimento e Avaliação Técnica de PRD de TI

O Gerente de Desenvolvimento e Avaliação Técnica de PRD de TI auxilia o Gerente de PRDde TI, proprietários de ativos de informação etc., fornecendo orientação na criação de planos adequados de PRD de TI e avaliando os requisitos técnicos para uma recuperação eficaz.

4.4.1 Atividades Chave:

- Projetar ferramentas de avaliação para determinar o nível apropriado de serviços de recuperação;
- Traduzir os requisitos de RD de TI em planos de RD, auxiliando as PAIs através do ciclo de vida de desenvolvimento do sistema de TI;
- Avaliar as capacidades de resiliência e recuperação e os riscos inerentes à infra-estrutura de TI;
- Correlacionar os requisitos de RD em Acordos de Nível de Serviço (SLAs), contratos e outros requisitos expressos (por exemplo, leis e regulamentos) com os planos de RD de TI;
- Promover o uso de novas tecnologias e processos em apoio a RD de TI.

4.4.2 Competências:

- Conhecimento especializado em PRD de TI;
- Experiência profissional de processos e prioridades comerciais críticas;
- Conhecimento prático de SLAs, contratos e memorandos de entendimento;
- Experiência profissional do ciclo de vida de desenvolvimento do sistema e gerenciamento do projeto;
- Capaz de projetar e desenvolver planos realistas de RD de IT

4.5 Escritório de RD de TI

Dependendo da quantidade de trabalho envolvido no gerenciamento dos planos e atividades de RD de TI, pode ser necessário um pessoal para dar suporte aos Gerentes de RD de TI. [Nota: o Escritório de RD de TI pode fazer parte do Escritório de PC anotado anteriormente, mas está mais

normalmente localizado dentro da função de TI, talvez dentro do Escritório de Gerenciamento de Projetos de TI].

4.5.1 Atividades Chave:

- Ajudar a construir um 'centro de excelência' para RD de TI - um ponto focal na organização oferecendo suporte e direção interna de consultoria em assuntos de RD de TI com a ajuda de gerentes de IT DR e outros especialistas;
- Manter inventários de sistemas de TI, serviços, etc., apoiando processos comerciais críticos;
- Programar e organizar reuniões para seus gerentes com os proprietários de ativos de informação e outros funcionários;
- Orientar e apoiar a criação de planos de RD de TI razoavelmente consistentes, abrangentes e de alta qualidade em toda a empresa, particularmente no que diz respeito a sistemas e serviços críticos de TI;
- Ajudar na elaboração de políticas, normas, procedimentos e diretrizes relacionadas a RD de TI;
- Executar ou apoiar outros na identificação e gestão de riscos relacionados a projetos de RD de TI;
- Auxiliar na criação de solicitações/propostas de orçamento, casos de negócios, etc., para diversas atividades de RD de TI;
- Monitorar e preparar relatórios gerenciais sobre os planos relacionados a RD de TI, progresso nos planos, orçamentos, riscos e oportunidades;
- Ajudar na coordenação e/ou entrega de atividades de conscientização, treinamento e educação relacionadas a RD de TI, exercícios/testes, etc;
- Ajudar em uma crise a implementar planos de RD de TI , abordar questões operacionais, comunicar clara e efetivamente, etc.

4.5.2 Competências:

- Conhecimento de trabalho de CN, RN, PC, PRD de TI etc.
- Capaz de construir e manter relações de trabalho produtivas com outros funcionários;
- Habilidades administrativas gerais, com alguma exposição ao gerenciamento de projetos, métricas/relatórios de gerenciamento, etc.
- Um olho para os detalhes, suficientemente diligente, persistente e eficiente para completar adequadamente as atividades designadas dentro de prazos realistas;
- Capaz de se comunicar com calma, eficácia e autoridade, inclusive em uma crise.

5 Outros papéis e responsabilidades relacionados ao PC

Várias outras funções de negócio normalmente desempenham papéis de apoio em relação ao GI, GC, PCN , PRN e PRD de TI. Embora eles possam não necessariamente apreciar sua relevância para o gerenciamento de contingência, após um incidente ou crise, espera-se que eles ajudem nas atividades de recuperação.

5.1 Papéis de Gerenciamento de Incidentes

O gerenciamento de incidentes é uma parte normal das operações comerciais rotineiras, por exemplo, lidando com pequenas interrupções, outros incidentes de segurança da informação e

quase-acidentes. Processos de gerenciamento de incidentes, papéis e responsabilidades, portanto, em sua maioria, estão fora da esfera do planejamento de contingência, exceto no caso de incidentes mais graves. Enquanto as atividades rotineiras de gerenciamento de incidentes provavelmente serão muito bem praticadas na corporação média, eventos excepcionais (tais como grandes incidentes físicos ou lógicos) podem exigir atividades diferentes que provavelmente não serão tão familiares e bem ensaiadas. Em particular, a gerência deve considerar a possibilidade de que o(s) gerente(es) de incidentes usuais possa(m) não estar(em) disponível(eis) durante ou após um incidente grave.

5.2 Papéis de Gerenciamento de Crise

Assim como no gerenciamento de incidentes, o gerenciamento de crises pode ser visto como uma extensão das atividades operacionais normais. Em circunstâncias normais, uma série de indivíduos são normalmente nomeados e treinados para cumprir rôles como, por exemplo:

- Gerente de Evacuação de Edifícios/Coordenador da Crise;
- Diretor de incêndio;
- Primeiro Ajudante;
- Guarda de Segurança Física/Site etc.
- Avaliador de Danos ou Líder da Equipe de Avaliação de Danos.

A organização deve assegurar que tais indivíduos estejam suficientemente bem preparados para agir adequadamente em circunstâncias excepcionais após um incidente grave, e que haja indivíduos treinados e preparados o suficiente para lidar razoavelmente bem com incidentes excepcionais (isto pode ser considerado como implicando a necessidade de treinamento básico de gerenciamento de crise para todos os funcionários, desde procedimentos típicos de evacuação de edifícios até combate a incêndios e primeiros socorros, quando apropriado).

5.3 Encarregados de Gerenciamento de Incidentes e Crises, planejamento de sucessão e rotação de trabalho

Além dos gerentes de incidentes primários e crises, o ideal seria que profissionais adequados fossem nomeados e treinados para assumir a liderança se o(s) gerente(s) primário(s) estiver(em) indisponível(eis) (esteja(em) envolvido(s) no incidente ou envolvido(s) de outra forma, por exemplo, em caso de doença, férias ou simplesmente sobrecarregado(s)). O planejamento da sucessão é recomendado para todos os papéis chave da organização, mas tem um significado especial em relação a incidentes graves. Algumas organizações, por exemplo, operam uma política deliberada de rotação de trabalho para expor múltiplos funcionários a tais papéis críticos, compartilhando conhecimentos e disseminando competências.

5.4 Proprietários de Ativos de Informação (IAOs)

Os "proprietários" de ativos de informação críticos, incluindo processos comerciais vitais, etc., têm um papel importante na especificação dos requisitos de disponibilidade (tanto de resiliência quanto de recuperação) como resultado do acompanhamento do processo AIN, e no financiamento dos controles associados. Enquanto que, a rigor, a entidade empresarial pode ser a proprietária legal de todos os ativos corporativos, os proprietários de ativos de informação (IAOs) dentro da organização são normalmente responsabilizados pessoalmente pela administração e outras partes interessadas pela proteção adequada dos ativos de informação sob sua alçada. Isto freqüentemente inclui ativos de informação pertencentes a terceiros, mas colocados aos cuidados da organização (por exemplo, dados pessoais relativos aos clientes).

Usando o processo AIN da organização, os IAOs se concentram nos aspectos CN da PC, tipicamente contando com custodiantes e especialistas em RD de TI para elaborar e fornecer os elementos RD de TI correspondentes. Eles planejam e coordenam as atividades da CN, especificam objetivos comerciais para a disponibilidade (normalmente em termos de resiliência,

objetivos de pontos de recuperação, objetivos de tempo de recuperação, etc.), alocam recursos para as atividades de CN e talvez de RD de TI, e avaliam os resultados dos testes de RD em relação às suas necessidades.

As competências da IAO incluem:

- Conhecimento profundo dos processos comerciais críticos sob sua responsabilidade, e uma compreensão razoável de sua priorização em relação a outros processos comerciais;
- Conhecimento prático dos sistemas de TI e outros recursos que apóiam seus processos comerciais críticos;
- Compreensão geral da PC, incluindo resiliência e RD de TI como aspectos complementares da PC;
- Conhecimento geral dos procedimentos de teste de RD de TI e exercícios necessários para fornecer garantia suficiente de que a resiliência e os arranjos de RD de TI satisfazem os requisitos de disponibilidade da organização;
- Conhecimento de trabalho do ciclo de vida de desenvolvimento dos sistemas de TI (de modo que os arranjos de RD de TI permaneçam alinhados com os requisitos da CN à medida que os sistemas de TI mudam);
- Capacidade de realizar a AIN, normalmente em conjunto com consultores especializados das equipes da BC/DRP, Gerenciamento de Risco, Gerenciamento de Segurança da Informação, etc.“

5.5 Custodiantes

Após a AIN, as responsabilidades relacionadas à operação e proteção/segurança dos ativos de informação que suportam processos comerciais críticos são normalmente delegadas aos Custodiantes, normalmente dentro do Departamento de TI para sistemas e redes de TI.

Embora os Custodiantes não sejam formalmente responsáveis por fornecer e provar a adequação do PRD de TI e outros acordos de contingência, eles têm o dever profissional de identificar e resolver questões em seu domínio de especialização e/ou trazer riscos residuais à atenção da gerência, incluindo os proprietários de ativos de informação, Gerentes de CN etc. Isto é especialmente importante no caso de configurações técnicas complexas de PRD de TI onde as pessoas de TI que estão familiarizadas com as tecnologias são mais propensas a notar problemas técnicos, dependências etc. que tornariam os arranjos ineficazes em um cenário de RD genuíno.

5.6 Funções operacionais de Continuidade de Negócios

Estas são as pessoas que operam processos comerciais mantidos ou restaurados em situações de contingência após incidentes e desastres. É mais provável que sejam funcionários comuns, mas alguns podem estar operando em áreas desconhecidas, por exemplo, cobrindo outros funcionários que são incapazes de trabalhar normalmente devido a ferimentos, incapacidade ou outra indisponibilidade.

Tais pessoas têm responsabilidades de se envolver ativamente em exercícios de PRD relevantes da Continuidade de Negócios e/ou TI, identificar questões não técnicas, dependências etc. que tornariam os arranjos ineficazes em um cenário de RD genuíno, e levá-los à atenção dos gerentes relevantes.

5.7 Funções das Operações de RD de TI

Estas são as pessoas que executam tarefas de recuperação de TI, tais como configurar sistemas de espera/recuperação para uso, restaurar backups de mídia offline, verificar os dados restaurados e liberar sistemas para uso em produção. Mais uma vez, é mais provável que sejam funcionários

comuns de TI, gerentes de rede/sistema, operadores, etc., mas podem estar operando em áreas desconhecidas, por exemplo, cobertura para outros funcionários de TI que não podem trabalhar normalmente devido a ferimentos, incapacidade ou outra indisponibilidade.

Os papéis de RD de TI abrangem muitas funções operacionais, por exemplo, administração de sistemas/aplicações, administração de banco de dados, rede e telecomunicações, aquisição, reabastecimento de servidores, Help/Service Desk de TI, etc.

Os papéis de RD de TI abrangem muitas funções operacionais, por exemplo, administração de sistemas/aplicações, administração de banco de dados, rede e telecomunicações, compras, reabastecimento de servidores, Help /Service Desk de TI, etc. Em tais papéis, os funcionários:

- Implementar os planos de RD de TI, tanto em testes como em incidentes reais;
- Avaliar a eficácia dos processos de RD de TI em testes e em eventos reais, fornecendo feedback e lições aprendidas para atualizar os planos.

As competências das Operações de RD de TI incluem:

- Conhecimento de trabalho de processos comerciais críticos, prioridades de recuperação e suporte a sistemas de TI, etc..;
- Conhecimento detalhado dos planos e procedimentos de RD para sistemas de TI etc. pelos quais têm responsabilidades de recuperação, além de conhecimento específico/especializado das plataformas de hardware associadas, sistemas operacionais, middleware, software aplicativo, configurações etc
- Capaz de identificar pontos fracos nos processos de RD e sugerir soluções realistas, por exemplo, como resultado de testes ou exercícios de RD.

6 Referências e leituras adicionais

Item	Relevância
BS 27999-1:2006 e BS 27999-2:2007	A British Standard 25999 parte 1, "Business Continuity Management Code of Practice", estabelece o processo, princípios e terminologia da gestão da continuidade dos negócios e fornece um conjunto abrangente de controles de melhores práticas de GCN cobrindo todo o ciclo de vida da GCN. A BS 25999 parte 2, "Business Continuity Management Specification", é uma norma mais formal de certificação BCM
PAS 77:2006	A Especificação 77, "Código de Prática de Gerenciamento da Continuidade dos Serviços de TI", disponível ao público, fornece orientação para garantir a continuidade dos serviços vitais de TI. .
NIST SP 800-34:2002	A Publicação Especial NIST 800-34, "Contingency Planning Guide for Information Technology Systems", fornece conselhos para medidas provisórias para recuperar serviços de TI do governo dos EUA após uma emergência ou interrupção do sistema.
ISO/IEC 27002:2005	A norma ISO/IEC "Tecnologia da Informação -- Técnicas de Segurança - Código de Prática para Gestão da Segurança da Informação" cobre a gestão da continuidade dos negócios na seção 14

7 Comentários sobre este documento

Você é encorajado a contribuir para o desenvolvimento e refinamento contínuo deste documento devolvendo comentários e sugestões de melhorias diretamente a seu autor (Gary@isect.com) ou discutindo-o através do Fórum de Implementadores da ISO27k em www.ISO27001security.com.

Embora não possamos notificá-lo se o documento for atualizado, tais atualizações serão normalmente divulgadas através da página do Kit de Ferramentas ISO27k em www.ISO27001security.com. Por favor, visite o site pelo menos uma vez por mês e/ou verifique a página "O que há de novo?" para obter detalhes de quaisquer atualizações

8 Agradecimento

Este documento foi baseado em um excelente documento de estratégia de treinamento em RD, gentilmente fornecido por Larry Kowalski, do Escritório de Programas de RD de Segurança Cibernética da Receita Federal dos EUA. Gary Hinson reformatou e ampliou ligeiramente o documento para os propósitos do kit de ferramentas ISO27k, mas permanece extremamente grato pela generosa contribuição intelectual que motivou este trabalho. Obrigado Larry!

Aviso de direitos autorais e isenção de responsabilidade

Como declarado na seção de escopo e aplicabilidade acima, este documento é um exemplo genérico para discussão e consideração. É muito pouco provável que este documento seja inteiramente suficiente ou adequado para qualquer organização específica sem personalização. Ele é de natureza genérica, incorporando uma seleção de rôles comuns e responsabilidades relacionadas ao planejamento de contingência em grandes organizações. Por ser genérico, não pode refletir totalmente as exigências de cada organização. Não estamos familiarizados com suas circunstâncias específicas e não podemos oferecer orientação sob medida para atender às suas necessidades particulares. Certamente não é aconselhamento legal e é improvável que reflita

plenamente quaisquer obrigações legais ou regulatórias sobre uma organização para preparar acordos de contingência adequados.